	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments	Error Definition
1	BRS	L9	8588	(group$1 WITH (access$6 OR obtain$6 OR acqui$6) WITH (information OR data OR database$1 OR memor$3 OR stor$4))	EPO; JPO; DERWENT	2002/04/07 20:35		
2	BRS	L10	29	9 AND ((encrypt$4 OR encipher$4 OR scrambl$4) NEAR4 (information OR data OR database$1 OR memor$3 OR stor$4))	EPO; JPO; DERWENT	2002/04/07 20:36		
3	BRS	L11	21	10 NOT us.pc.	EPO; JPO; DERWENT	2002/04/07 20:37		
4	BRS	L12	6	11 AND (@pd<19990301)	EPO; JPO; DERWENT	2002/04/07 20:37		

	Errors
1	0
2	0
3	0
4	0

CLIPPEDIMAGE= JP411015373A
PAT-NO: JP411015373A
DOCUMENT-IDENTIFIER: JP 11015373 A
TITLE: OPEN KEY CODING SYSTEM

PUBN-DATE: January 22, 1999

INVENTOR-INFORMATION:
NAME
AOKI, RYUICHI

ASSIGNEE-INFORMATION:
NAME COUNTRY
FUJI XEROX CO LTD N/A

APPL-NO: JP09164506
APPL-DATE: June 20, 1997

INT-CL (IPC): G09C001/00; G09C001/00 ; G09C001/00 ;
H04L009/08

ABSTRACT:
PROBLEM TO BE SOLVED: To share the coded information between members in a group while securing the sophisticated secrecy by combining the encryption of the plain text by an arbitrary member belonging to the group with the group public key generated as the group unit.

SOLUTION: The group public key PG and the group secret key SG to be allotted with the group consisting of one or more members as the unit, and one or more encrypted group secret keys PM<SB>i</SB>(SG) (i=1-n) in which the data of the group secret key SG is converted and encrypted, are provided. The **group** secret key SG is **obtained** by decrypting the encrypted **group** secret key PM<SB>i</SB>(SG) by the member secret keys SM<SB>i</SB> specific to each member, and the **encrypted information by the group** public key PG is decrypted using the **obtained group** secret key SG.

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments	Error Definition
1	BRS	L1	13472	(group$1 WITH (access$6 OR obtain$6 OR acqui$6) WITH (information OR data OR database$1 OR memor$3 OR stor$4))	USPAT	2002/04/07 19:02		
2	BRS	L2	658	1 AND ((encrypt$4 OR encipher$4 OR scrambl$4) NEAR4 (information OR data OR database$1 OR memor$3 OR stor$4))	USPAT	2002/04/07 19:03		
3	BRS	L3	73	2 AND (group$1 WITH (password$1 OR challeng$4 OR handshak$4 OR (hand ADJ1 shak$4)))	USPAT	2002/04/07 19:04		
4	BRS	L4	2	3 AND (group$1 NEAR4 ((public ADJ2 key) OR (private ADJ2 key)))	USPAT	2002/04/07 19:04		
5	BRS	L6	0	5 AND (((encrypt$4 OR encipher$4 OR scrambl$4) NEAR4 (number OR value OR sequence OR bitsequence)) WITH (public ADJ2 key))	USPAT	2002/04/07 19:06		
6	BRS	L5	16	3 AND (((encrypt$4 OR encipher$4 OR scrambl$4) NEAR4 (information OR data OR database$1 OR memor$3 OR stor$4)) WITH (number OR value OR sequence OR bitsequence))	USPAT	2002/04/07 19:28		

	Errors
1	0
2	0
3	0
4	0
5	0
6	0

	Type	L #	Hits	Search Text	DBs	Time Stamp	Comments	Error Definition
7	BRS	L7	255	2 AND (group$1 WITH (pin$1 OR identif$6 OR password$1 OR challeng$4 OR handshak$4 OR (hand ADJ1 shak$4)))	USPAT	2002/04/07 19:27		
8	BRS	L8	82	7 AND (((encrypt$4 OR encipher$4 OR scrambl$4) NEAR4 (information OR data OR database$1 OR memor$3 OR stor$4)) WITH (number OR value OR sequence OR bitsequence))	USPAT	2002/04/07 19:29		

	Errors
7	0
8	0

DOCUMENT-IDENTIFIER: US 5764890 A
TITLE: Method and system for adding a secure network server to an existing
computer network

---------- KWIC ---------

ABPL:
A method and system for adding a secured network server to an existing network
for access by a client thereof, wherein the added server does not possess a
database of authentication credentials. The client is first authenticated for
access to the added server by passing authentication requests received from the
client to an authenticating agent having a **database** of authentication
credentials, which may include **information** from a bindery comprising users,
groups and passwords. The responses from the authenticating agent are then
evaluated, and if the response indicates validity, the client is the granted
access to the added server. Database services are provided to the
authenticated client by first evaluating database requests received from the
client. Requests seeking information maintained by the authenticating agent
are handled by passing the requests to the authenticating agent and using its
response to reply to the client.

BSPR:
Verification is performed by the server, which references an internal database
of authentication information including the user's password (**stored in**
encrypted form) to similarly calculate the expected encrypted combination code.
If the combination code received by the server matches the code calculated by
the server, and other restrictions (such as login hours) are satisfied, the

client is admitted to the system. In this manner, only users in possession of
a correct password are allowed to login to the server.

BSPR:
Access rights are typically organized by groups of users, and thus such secured
devices also maintain a list of groups that the user belongs to. The list of
valid users, their associated **passwords, group** information and other related
detailed information is maintained in a database on the server, sometimes
referred to as the bindery.

BSPR:
Briefly, the invention provides a method and system for adding a secured
network server to an existing network for access by a client thereof, wherein
the added server does not possess a database of authentication credentials.
After connecting to an authenticating agent having a **database** of authentication
credentials, which may include **information** from a bindery comprising users,
groups and passwords, the client is first authenticated for **access** to the added
server by passing authentication requests received from the client to the
authenticating agent. The responses from the authenticating agent are then
evaluated, and if the response indicates validity, the client is the granted
access to the added server.

DEPR:
The client 22 utilizes the challenge key to internally encrypt its password,
and sends the encrypted password to the network server 24 at step 11 within a
login request. However, since the network server 24 does not want to login to
the authenticating agent 26 with these credentials, the network server first
converts the login request to a verification request instead of passing the
login request to the authenticating agent 26. After the

conversion the
verification request is sent (step 12). The authenticating agent 26 verifies
the password with its authentication **database 26.sub.b by performing an**
analogous encryption using the challenge key it previously sent to the client
22 via the network server 24.

DEPR:
Although not necessary to the invention, so that the network server 24 does not
need to further communicate with the authenticating agent 26 each time a
request is made by authorized clients connected thereto, the network server 24
maintains its own list of groups that each user belongs to, which provides
information on which of its own services are available to the users and/or user
groups based on their rights. This list is obtained at the time of the login,
and remains valid for the duration of the session for use in access control.
Alternatively, it is feasible to update the list of user's **group** memberships
while the user is logged in, such as by having the network server 24
periodically request and **obtain** an updated list of users and user **groups** from
the remotely located authentication **database** 26.sub.b of the authenticating
agent 26.

DEPR:
As previously described, the authenticating agent 26 typically comprises a
Novell.RTM.-based NetWare.RTM. server including a database 26.sub.b therein,
also known as a bindery or bindery emulation (FIGS. 2 and 3). The database
26.sub.b contains lists of network resources, valid users, and associated user
information, including an associated **password stored in encrypted** form for each
user, and a list of **groups** to which the user belongs. The authenticating agent

26 also includes the encryption scheme 33 that conforms to the encryption
algorithm 30 present in the client device 22 (FIG. 4).

DEPR:
Significantly, the network server 24 does not possess any authentication
information. Thus, when dealing with users, **passwords or groups** the network
server must communicate with the authenticating agent 26. The network server
24 does possess a local database (bindery) 24.sub.b of its own for maintaining
certain local objects such as printer services and print queues, but it is only
a partial bindery because it does not contain user objects, **group** objects, or
passwords.

DEPR:
The received reply packet 440 to the "Get Encryption Key" request is similar to
the "Get Bindery Object ID" reply packet 390 of FIG. 8D, except that the packet
sequence number in field 442 is now appropriately returned as 03h, and the **data**
in field 448 now contains the encryption key.

DEPR:
In keeping with the invention, at step 526 of FIG. 5A, the network server 24
copies the received reply packet 440 and transmits it to the client workstation
22. FIG. 8H represents the pre-copied reply data packet sent from the
authenticating agent 26 to the network server 24, while FIG. 8I represents the
post-copied reply data packet sent from the network server 24 to the client
workstation 22. As before, fields 441 (FIG. 8H) and 451 (FIG. 8I) both
identify their respective packets as reply packets by being set equal to 3333h.
Field 442 returns a packet sequence number of 03h since that was the sequence
number sent by the network server 24 to the authenticating agent 26, while
packet sequence field 452 returns 04h to the client

workstation 22. The
connection numbers returned from the authenticating agent 26 are adjusted by
the network server 24 to the appropriate values for the client workstation 22,
i.e., from 0048h in fields 443, 445 (FIG. 8H) to 0005h in fields 453 and 455
(FIG. 8I). The completion code (00h) is not changed from field 446 to field
456, nor is the **encryption key changed from data** field 448 to data field 458.

DEPR:
In keeping with the remote authentication aspect of the invention, the network
server 24 translates the **data packet and passes the encryption** code therein to
the authenticating agent 26 for verification at step 542 of FIG. 5B. However,
unlike previous packets, during this particular translation the network server
24 also modifies the requested function of the request packet. This is because
the network server 24 is not actually logging into the authenticating agent 26
with the client's credentials, but is instead only verifying the client's
credentials. Accordingly, instead of sending a "Login Object Encrypted"
request packet to the authenticating agent 26, the network server translates
the login request packet to a "Verify Bindery Password Object Encrypted"
request packet.

DEPR:
To this end, the network server 24 changes the subfunction code from a value of
18h in field 468 of FIG. 8J to a value of 4Ah in field 478 of FIG. 8K. The
function code of 17h in fields 466 and 476 remains unchanged. As previously
described, the other fields are modified as necessary for transmission to the
authenticating agent. As also previously described, the translated request
keeps the data portion of the packet intact (fields 469-472, FIG. 8J), and thus

the **encrypted password and related information** is transmitted to the authenticating agent 26 without modification (step 544 of FIG. 5B). The related information in fields 470-472 includes the object type, the length of user name and user name "JOE."

DEPR:
However, while a connection is present, the network server 24 is further able to perform a number of additional functions that require **access** to the user and **group** objects maintained in the **database** 26.sub.b of the authenticating agent 26. Thus, in accordance with another aspect of the invention, the server 24 is able to provide users with a number of database (bindery) services commonly available to users logged into servers having a complete bindery.